Inspira-Journal of Commerce, Economics & Computer Science (JCECS)
(A National bi-lingual Quarterly Double Blind Open Access Peer Reviewed Refereed Journal)
ISSN : 2395-7069(Print), Impact Factor: (Cosmos 7.650 & I2OR 5.120), Volume 12, No. 03, July-September, 2026, pp. 221-230

Digital Financial Literacy and Susceptibility to Online Financial Fraud among Working Women in Delhi- NCR: The Mediating Role of Protective Financial Behaviour and Financial Confidence

Dr. Jagveer Singh[1*] & Jyoti Chauhan[2]

[1]Assistant Professor, NREC Collage Khurja, Bulandshshr, Uttar Pradesh, India.
[2]Research Scholar, NREC Collage Khurja, Bulandshahr, Uttar Pradesh, India.

[*]Corresponding Author: jyoti909chauhan@gmail.com

Citation: *Singh, J. & Chauhan, J. (2026). Digital Financial Literacy and Susceptibility to Online Financial Fraud Among Working Women in Delhi- NCR: The Mediating Role of Protective Financial Behaviour and Financial Confidence. Journal of Commerce, Economics & Computer Science, 12(03), 221–230. https://doi.org/10.62823/jcecs/12.03.9542*

Abstract

The tremendous growth of digital wallets, mobile banking, internet banking, Unified Payments Interface (UPI) and digital payment systems has been phenomenal disruption in Indian financial ecosystem. These developments have enhanced transactional efficiencies and financial inclusion but have also exposed people to sophisticated online financial frauds such as phishing, vishing, identity theft, QR-code scams, fake investment schemes and social engineering attacks. Our increasing reliance on digital banking has changed financial literacy from traditional budgeting, saving and investing to the ability to identify digital hazards, evaluate online financial data and practice safe financial practices. Working women are a very important group of people in this changing environment. As women's participation in the workforce, financial independence and reliance on digital services have increased, so too have their prospects and vulnerability to cyber-enabled dangers. Research shows that while inclusion has improved, women still tend to be more risk averse, less confident about their finances and have varying levels of digital skills, all of which can make them more vulnerable to fraud. There has been little attention paid to the behavioral processes through which digital financial literacy contributes to fraud protection, whereas existing studies discuss financial literacy in relation to savings, investment behavior or financial well-being. The current study has conceptualized Digital Financial Literacy as the primary predictor of Online Fraud Vulnerability with Protective Financial Behavior as the mediating variable and Financial Confidence as a significant psychological determinant based on the theory of planned behavior and protection motivation theory. It recommends to do research based on the review of current literature of working women in NCR who regularly make use of digital financial services. This study contributes to the existing literature by redefining digital financial literacy to include fraud detection and cyber-risk awareness, in addition to financial knowledge and digital competence, and provides practical recommendations for regulators, employers, financial institutions, and legislators to enhance the digital financial resilience of women.

Keywords: *Digital Financial Literacy, Online Financial Fraud, Working Women, Protective Financial Behaviour, Financial Confidence, Behavioural Finance, Financial Inclusion, Structural Equation Modelling.*

Introduction

The way people access, manage, and utilize financial goods has changed globally due to the digital transformation of financial services. The adoption of digital financial services has accelerated due to advancements in financial technology (FinTech), increased internet penetration, and smartphone

[*] *Copyright © 2026 by Author's and Licensed by Inspira. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work properly cited.*

access. This has made transactions quicker, easier, and more accessible. Initiatives like Digital India, Jan Dhan Yojana, Aadhaar-enabled services, and the Unified Payments Interface (UPI) helped accelerate this change in India by lowering financial access barriers and encouraging cashless transactions among urban and semi-urban populations.

With billions of transactions processed each month, UPI has emerged as one of the fastest-growing digital payment systems in the world, according to the National Payments Corporation of India (NPCI). Mobile banking, internet banking, digital wallets, and investment applications have become integral to consumers' daily financial activities, extending beyond routine payments to savings, insurance, investments, lending, taxation, and wealth management, thereby increasing the complexity of financial decision-making.

However, new vulnerabilities have been created by this quick expansion. Online fraud involving phishing emails, fraudulent links, phony customer care services, QR code manipulation, identity theft, SIM swapping, malware, remote-access programs, phony investment platforms, and social engineering has sharply increased due to the increasing expertise of hackers. In contrast to traditional fraud, digital fraud frequently takes use of cognitive limits, behavioural biases, and a lack of cyber-security awareness in addition to technological flaws. Consequently, people may fail to fail to fail to recognize basic security.

This panorama has widened the concept of financial literacy. In the past, it meant comprehending risk diversification, savings, investment planning, inflation, compound interest, and budgeting. These are still necessary, but in a digitally connected economy, they are insufficient. Modern financial competence increasingly necessitates that people assess the legitimacy of digital platforms, comprehend cyber-security procedures, protect credentials, spot fraudulent communications, and make wise choices in technologically enabled contexts.

Digital financial literacy, which combines financial knowledge with digital competence, cyber-risk awareness, and secure behavior, has so evolved as an extension of traditional financial literacy.

Working women make up a particularly sizable portion of the groups involved in India's digital economy. Women are adopting digital services for salary management, household expenditures, investments, insurance, and personal financial planning as a result of increased educational attainment, increased labour force participation, growing earnings, and increased financial autonomy. However, there has been advancements in the cyber-matched.

Prior research frequently reveals gender variations in financial knowledge, investing confidence, and decision-making. Despite exhibiting similar skills when provided with sufficient information, women report lower levels of financial confidence than men. Additionally, they typically show less risk tolerance and more caution, traits that, depending on the type of fraud, may either enhance or decrease vulnerability. Depending on the presence of excessive trust in perceived authority, lack of verification, low awareness of evolving approaches, or, alternatively, overconfidence in one’s digital skills, susceptibility may take on different forms.

In the existing literature, financial literacy has been studied according to inclusion, investment decisions, retirement planning, savings or well-being. There is little research on the impact of digital financial literacy on the ability to recognize and resist fraud, and even less on the behavioral processes through which knowledge translates into protective action. Knowing doesn't make you behave securely, just as accessing online services a lot doesn't mean you are good at resisting fraud. The line between digital adoption and digital safety is still under explored especially in the Indian context.

Another gap is financial confidence. Proper confidence promotes informed engagement and independent decision-making, whereas excessive confidence can breed complacency, heuristic reasoning, and increased vulnerability to elaborate schemes. In contrast, a lack of confidence may prevent independent assessment and increase dependence on fallacious advice. The question of whether financial confidence is a protective or a vulnerability factor is yet to be resolved.

The present study fills these gaps by proposing an integrated conceptual model linking Digital Financial Literacy, Protective Financial Behavior, Financial Confidence and Online Fraud Vulnerability among working women in Delhi-NCR. Drawing on the Theory of Planned Behavior and Protection Motivation Theory, it argues that digital financial literacy improves protective behavior by reinforcing perceived behavioral control, threat appraisal and coping mechanisms, thus reducing fraud vulnerability. As a psychological factor, financial confidence is considered as a variable that may either strengthen

protective behavior or increase vulnerability, depending on how far it is a true reflection of actual competence. The research shifts the discussion from financial inclusion to financial resilience and provides insights for policymakers, regulators, financial institutions and employers and educational organizations designing evidence-based programs that enhance digital safety as well as inclusion.

Literature Review

- **Digital Financial Literacy: Concept and Evolution**

Financial literacy is the ability and knowledge to make good decisions about borrowing, investing, saving, and asset management. That's the classic definition. With the rapid digitization of financial services, this notion has expanded to include the skills needed to securely access, assess and use digital products. The emergence of internet banking, mobile payments, digital wallets, FinTech applications and AI-driven services has transformed the interactions of consumers with financial institutions, and academics and policymakers have emphasized the concept of digital financial literacy (DFL) as a multi-dimensional concept that combines financial knowledge with digital competence, cyber-security awareness and responsible behavior.

This view has been largely formalized thanks to the OECD. The OECD/INFE Survey Instrument to Measure Digital Financial Literacy (2024) defines digital financial literacy (DFL) as "the combination of knowledge, skills, attitudes and behaviors that enables individuals to use digital financial services safely and productively while maintaining their financial well-being." Unlike the traditional approaches, the framework covers cyber-security protocols, online authentication, fraud detection, privacy protection, and responsible application of digital technologies.

Over a third of adults still lack the minimum skills to identify digital risks, verify online information and practice online safety; those with higher DFL consistently reported greater resilience to financial shocks and safer online behavior. The proliferation of UPI, digital banking and mobile based services has made DFL an essential part of inclusion in India. In an empirical study of Indian women, Mishra, Agarwal, Sharahiley, and Kandpal (2024) argued that digital competence directly supports women's empowerment and economic participation. DFL greatly improves decision-making by enhancing users' capacity to assess products, comprehend risks, and confidently participate in technology-enabled markets. Taken as a whole, these studies suggest that DFL extends far beyond an understanding of how payment apps work to incorporate the ability to analyze information critically, recognize fraudulent messages, protect credentials, and make safe judgments in complex digital environments.

Online Financial Fraud in the Digital Economy

The surge in digital financial crimes has happened contemporaneously with the boom in digital services. The focus of fraud has shifted from exploiting systemic and structural vulnerabilities to behavioral vulnerabilities with phishing, vishing, malicious customer care services, QR code manipulation, identity theft, remote access applications, Ponzi and Pyramid schemes, and social engineering.

The OECD (2026) identifies the rapid rate of digitalization, low levels of DFL, and sophistication of fraud techniques as the primary factors that fuel global financial fraud. The OECD contends while the innovation has improved accessibility, it has created a complex environment for consumers to make security judgments. To mitigate fraud, the OECD asserts a holistic approach of enhancing technological safeguards in conjunction with behavioral and digital awareness is required. Fraudsters operating in the Indian market use the same methods and elaborate schemes to defraud consumers of their money. In the process, they expose the banking system and payment systems to fraud. User behavior in the digital economy is often the weakest link. Without sufficient behavioral capability and awareness in digitally enabled financial security systems, threats are likely to persist.

Digital Financial Literacy and Fraud Vulnerability

One ongoing research area explores whether increasing financial literacy lessens susceptibility to online fraud. With traditional literacy, the link with decision making has been well-documented, however, with online fraud victimization, the body of research remains limited.

The study by Isaia, Oggero and Sandretto (2024) is the most comprehensive study on the subject, and is based on a representative sample of the Italian population. The study found that objective financial literacy protected against online fraud, and that subjective financial overconfidence increased

the risk of online fraud victimization. The authors stated that financial literacy acted as a protective factor, only when accompanied by a realistic self assessment and cautious approach. The authors' findings are in line with OECD research which states that individuals, who are competent in utilizing digital financial literacy, recognize and interpret risks, and adopt safer digital financial practices. Within India, studies focusing on the relationship between DFL and online fraud victimization are still lacking. Research in this area focuses primarily on DFL and financial inclusion and payments.

Protective Financial Behaviour as a Behavioural Mechanism

Behavioural theories describe why transforming knowledge into action sometimes fails. The Theory of Planned Behaviour (Ajzen, 1991) states that attitudes, subjective norms, and the individual's perception of control affect behaviour. With regard to security behaviour, individuals with greater perception of control are likely to practice protective security behaviours. Protection Motivation Theory (Rogers, 1975; Maddux & Rogers, 1983) proposes that self-protective behaviours are enacted when an individual perceives a threat to be serious, and is capable of responding to it. In the context of digital finance, these behavioural theories argue that the absence of DFL creates fraud vulnerability; however, the presence of DFL impacts fraud protection, directly (i.e. by practicing protective behaviours) and indirectly (i.e. by influencing an individual's perception of security and control). According to the OECD policy reports, individuals who adopted secure behaviours to manage their digital finance exposure, such as by practicing secure password management, avoiding financial transactions over public, unsecured Wi-Fi, and verifying payment requests, were less exposed to fraud. Protective behaviour thus acts as the mediating factor that connects DFL to fraud resistance.

Financial Confidence and the Risk of Overconfidence

Financial confidence is a measure of how much one believes in himself or herself in terms of making effective decisions. In behavioural finance, there is a distinction made between well-calibrated confidence, which leads to good decision-making, and overconfidence, which often leads to risky behaviour and lowered alertness. The study carried out by Isaia et al. (2024) clearly shows that overconfidence leads to a higher possibility of being victims since those people who had been overconfident of their ability ignored warnings and trusted fraudulent emails while underestimating the risks. Studies related to women show that women consumers are generally less confident but equally capable when enough information is provided to them. According to Mishra et al. (2024), improvement of DFL will lead to higher levels of confidence in women, which will enhance decision-making and economic engagement of women.

Digital Financial Literacy among Working Women

The participation of women in formal employment has increased their interaction with digital services. Payments for salaries, investments, insurance, taxes, and other transactions are being done through digital channels, thus making professionally working women a significant part of the economic ecosystem in India. Nonetheless, the earlier research has mostly concentrated on the financial literacy of women from the perspective of inclusion, saving, entrepreneurship, and investment decisions without giving due consideration to their preparedness to detect and resist any fraud. According to Mishra et al. (2024), DFL positively impacts the decision-making process of women by improving their access to information, building their confidence, and providing independence, but only in regard to financial decisions, not fraud prevention.

Research Gap

The literature review has revealed several gaps. First of all, there is a conceptual gap in this topic because the overwhelming majority of researchers measures DFL through digital adoption or use but not the capability to recognize, evaluate and resist fraud. Secondly, there is a behavioral gap since there is a lack of empirical studies that examine the mediating role of protective financial behavior. Thirdly, there is a psychological gap concerning financial confidence, which can be viewed as both a protective and vulnerable characteristic. There is also a methodology gap because very little work has been done using SEM to analyze the relationship between DFL, protective behavior, confidence, and vulnerability to fraud. To address these gaps, this paper offers an integrated behavioral theory based on the Theory of Planned Behavior and Protection Motivation Theory.

Digital Financial Landscape in India: Opportunities and Emerging Risks

- **India's Digital Financial Revolution**

India has become a frontrunner in the digital economy, owing to FinTech innovation, adoption of smartphones, low-cost Internet, and proactive policies of the government. During the last ten years, there has been a change from transactions being carried out in cash form to digital transactions supported by the Digital India Initiative, the Pradhan Mantri Jan Dhan Yojana (PMJDY), Aadhaar-based services, and the UPI system, which together contribute to the formation of an advanced Digital Public Infrastructure that improves access to financial services.

The launch of UPI in 2016 by NPCI was a milestone moment, as it facilitated instant transfers of money via phones and made banking less complicated. The user-friendly and cost-effective nature of the system contributed greatly to its widespread use. As per the Reserve Bank of India (2024), the volume of transactions conducted via digital methods has increased exponentially, with a significant share coming from the UPI system.

Mobile banking, internet banking, digital wallets, QR code payment mechanisms, and contactless systems have become an essential part of everyday functioning.

The developments in the area have brought about several advantages: increased inclusion of people, lower transaction costs, greater transparency, cashless transactions, and direct welfare benefit payments. The fast development of the FinTech industry has brought about digital lending, robo advisory services, online investment platforms, P2P lending and digital insurance, thus integrating financial services into the lives of consumers more fully. Digital services have proved valuable for women in such areas as management of salary, family expenses, investments, insurance, paying taxes, and making plans for retirement. This happened because of several projects aimed at increasing inclusion of women.

However, digital inclusion does not mean digital literacy. Most people are unfamiliar with the issues of cyber security, fraud detection and proper behavior in the Internet environment. The convenience of transaction processes has become greater than the ability to detect fraud and protect oneself.

- **The Growing Threat of Online Financial Fraud**

Alongside the rapid growth in digital services, there has been a corresponding increase in levels of fraud. As the volume and complexity of transactions increases, criminals have adapted to take advantage of the psychology of behaviour, lack of technology knowledge, and asymmetric information, using psychological persuasion and social engineering tactics rather than direct theft or hacking.

Online fraud refers to deceitful actions that seek to gain unauthorized access to financial information, credentials, or assets. Such types of fraud include phishing, vishing, smishing, QR-code scams, false KYC verification, fraudulent customer support, impersonation of financial institutions, remote-access frauds, identity theft, online investment platform frauds, cryptocurrency scams, and employment fraud. Through the application of artificial intelligence technology, deep-fakes have been possible, leading to difficult-to-detect fraudulent messages. The common feature among such types of frauds is the use of psychological persuasion as fraudsters exploit the fears, urgency, and greed of individuals to force them to provide OTPs, click on links, scan QR codes, download remote-access software, and make transfers.

Cyber fraud has risen sharply in India. Reports have been issued by the RBI, Ministry of Home Affairs, National Crime Records Bureau, and Indian Cyber Crime Coordination Centre regarding cases involving payment frauds, identity fraud, unapproved transactions, and investment scams. The human aspect is still considered to be one of the most vulnerable parts of the ecosystem. The impact of fraud not only leads to financial losses but also psychological trauma, a loss of confidence, decreased propensity to use technology, and insecurity.

- **Working Women in India's Digital Financial Ecosystem**

Working women make up one of the rapidly growing demographic groups among users. Growing participation in the workforce, education level, availability of banks and finance, and independence have been driving active involvement in digital technologies related to payments, household costs, investing, insurance, taxation, and other transactions. Digitalization has provided women with benefits in the form of convenience, decreased use of cash, decision-making independence, and increased access to formal products, providing flexibility needed by working women.

But increased activity leads to increased exposure to risk. Working women usually perform transactions under pressure of time, perform multiple activities simultaneously, and use mobile technology, which might be making them more vulnerable to communication that requires immediate response. Differences in digital literacy and cyber security awareness will affect the way women perceive suspicious communication. Women tend to have lower subjective digital literacy even in cases when their actual competences are equal; being cautious might help avoid some risks but lacking confidence could prevent verification of communications, whereas overconfidence could decrease attention to the situation.

- **Behavioural Perspectives on Fraud Vulnerability**

With regard to how advanced online frauds are becoming, there is a focus on vulnerabilities associated with people's behaviors rather than security problems in technology. It has become rare for the success of online frauds to depend solely on technological vulnerabilities; the reason is that they take advantage of predictable behavioral patterns of the human mind. The principles of behavioral finance and consumer psychology shed light on why people with identical information behave differently.

There are various biases that make people vulnerable to online fraud. The authority bias makes people susceptible to believing any kind of communication they receive from their bank, the government or police. Urgency bias encourages people to act without verifying anything when the fraudster tells them that they might lose access to their accounts if they do not do something. Social proof makes people believe when the message suggests that other people have already acted in that situation. Loss aversion encourages people to make unnecessary sacrifices in order to avoid losing something. Confident people are vulnerable due to overconfidence bias and confirmation bias.

- **Digital Financial Literacy as a Protective Mechanism**

The growing number of digital services has changed the concept of inclusion from issues of access to questions about capability. Although platforms have enabled many people to engage in the formal sector, their use has created some new risks that make the capacity to navigate these digital spaces a vital life skill. This has increased the meaning of financial literacy from knowledge to skills of being digitally literate, aware of the cyber risks and behaving protectively. The existing research has explored the DFL as a factor of inclusion, payment adoption, investments and well-being without much regard for the way it creates a protection resource. It is suggested that DFL should not only be considered as knowledge acquisition but as a capability that enables a person to identify the threat, assess the information and adopt a protecting behaviour.

- **Understanding Digital Financial Literacy**

DFL goes beyond being familiar with apps and involves the competencies of knowledge, skills, attitude, and behavior required for accessing, assessing, utilizing, and safeguarding the digital products responsibly. Based on the OECD/INFE model, this research outlines five interconnected dimensions. Financial Knowledge entails the understanding of simple concepts, such as budgeting, interest rate, inflation, saving, investing, insurance, and risk diversification. People with good knowledge are better placed to spot the unrealistic claims that are always made in frauds. Digital Competence refers to technical competence in operating apps, such as banking apps, payment systems, and using biometrics and two-factor authentication among others. Cyber Security Awareness is the competency of spotting the dangers and adopting the safe practices, such as phishing, fraud websites, suspicious links, and QR codes among others. Critical Evaluation Skills allow consumers to crosscheck sources, evaluate their credibility, and be able to differentiate between real prospects and scams, and make sure that no hasty decisions are made on the basis of inaccurate information obtained from various forms of communication such as social media, advertisements, and applications. Responsible Financial Behaviours refer to using the information to perform certain actions that include protecting passwords and OTPs, software updates, checking of financial statements, secure connections, and notifying authorities.

- **Protective Financial Behaviour: Translating Knowledge into Action**

One of the key arguments in this regard is that knowledge alone does not guarantee safety. People may have full knowledge of cybersecurity but still practice unsafe behaviors as a result of convenience, habits, time constraints, misplaced trust, and biases. The efficacy of DFL will depend on whether people are able to consistently engage in protective behaviors such as verification of payments, denial of credentials, multi-factor authentication, creation of strong passwords, updates of applications, avoidance of unknown links, and verification of suspicious communication.

The Protection Motivation Theory provides an explanation of why people engage in protective behavior as long as they realize the severity of the danger faced and the capability to respond. People with high levels of DFL tend to recognize the dangers, comprehend the consequences, and perceive that preventive measures decrease the probability of facing any harm. Also, according to the Theory of Planned Behavior, protective behavior depends on attitudes toward security, perceived behavioral control, and subjective norms.

Financial Confidence: A Double-Edged Psychological Construct

Financial confidence refers to how well an individual believes he or she can make decisions. Financial confidence leads to decision-making, makes an individual willing to get involved in market activities, and helps him or her avoid seeking informal advice, but it is good only if it is accurate. Well-tuned confidence makes one be able to assess information critically, ask questions about suspicious queries, check any transactions and implement any necessary preventive measures. On the contrary, too much confidence might make one vulnerable. People who overvalue their skills tend to under value the risks associated with them and tend to disregard warnings, security measures and also tend to believe that frauds will not affect them. Fraudsters use this weakness to lure people through creating a believable scam. People with low confidence may also be vulnerable as they may not ask questions and may seek too much advice from the outside world. Financial confidence should thus align with the ability to make good decisions.

A Conceptual Framework for Fraud Vulnerability Among Working Women

DFL has been proposed within the framework as the underlying cognitive ability that affects the individuals' reaction to risk in terms of their behavior and psychology. Higher DFL is associated with the increased awareness of individuals, as well as their critical thinking skills and comprehension of the safe behaviors. Those abilities are implemented through Protective Financial Behavior (PFB), which has been designated as the main behavioral approach used to decrease exposure, since the actual implementation of knowledge rather than knowledge per se is necessary for the reduction of exposure. Additionally, the concept of Financial Confidence (FC) is introduced within the framework as the independent psychological factor affecting both the protective behavior of individuals and their vulnerability to fraud online. The appropriate level of confidence helps people make informed decisions, while excessive confidence might lead to negligence.

Thus, the framework could be presented as follows:

- Digital Financial Literacy (DFL) → Protective Financial Behavior (PFB) → Online Fraud Vulnerability (OFV)
- where Financial Confidence (FC) affects both PFB and OFV.

An Integrated Behavioural Perspective

It is not possible to account for the reasons behind online fraud with technological or monetary factors alone. Vulnerability arises due to the interaction of three things – cognitive ability, behavior and psychological traits. DFL equips an individual with awareness regarding any risk involved; behavior implements the awareness in day-to-day activities; and confidence determines how one will interpret the information received and respond to the risks involved. In case of working women, it gains even more importance as the role of women is increasing. Improving DFL should go beyond mere knowledge building to include safe behavioral patterns and confidence.

Policy Implications and Recommendations

The growth of the digital economy of India has led to opportunities of empowerment and inclusion, but the concomitant increase in fraud calls for a holistic strategy for digital capabilities. The issue of DFL needs to be seen not just in terms of education, but as an important element of consumer protection and cybersecurity that needs cooperation from all stakeholders including the consumer.

Government and Financial Regulators

However, regulation by entities such as the RBI, SEBI, NPCI, and the Ministry of Electronics and Information Technology is key but the complexity of fraud calls for moving from an awareness campaign to behavioural capability. Firstly, there is need for explicit integration of DFL into national programmes on financial literacy that include topics on phishing, checking QR code, passwords, digital identity protection,

investment fraud, AI-based fraud and application safety. Secondly, there is a need for regulatory bodies to encourage behaviour nudging through platforms such as timely warning on security issues, fraud alerts, etc., to avoid impulse in risky transactions. Thirdly, coordination of regulators, cyber-security bodies, telecom companies and law enforcement is vital for swift detection and response. Lastly, there is a need for developing gender-sensitive measures that take into consideration the special role of women.

Banks and Financial Institutions

As the main interface between customers and services, the banks need to transcend from messaging to constant education using interactive programs, phishing simulations, mobile training, and multilingual training. Machine learning and AI technology can be used in improving fraud detection through monitoring, anomaly detection, geolocation, and authentication. Banks should also make the process of reporting easier since the victims may take time reporting because of complicated processes involved, and personalized training for each group as some groups such as women and elderly people face unique threats.

Employers and Corporate Organizations

Since the companies are pushing for digitalization of payment of salaries, refunds, tax payment and benefits, the companies can improve their employees' capabilities by integrating DFL in the wellness program, which could be in the form of seminars on cybersecurity, safe payments, investment fraud, and identity theft. Collaboration with banks, cybersecurity experts, and educators would help in showcasing how the latest technology works, particularly the female employees.

Educational Institutions

The inclusion of the DFL in academic institutions, regardless of subject matter, is an absolute must, and the course should not only be theoretical but also impart the skills needed to handle online banking security, proper payments usage, identify fraud, and investment safety. The use of experiential methods, such as case studies, simulations, role-playing, and even awareness campaigns, would be beneficial. Behavioural finance principles need to be taught in business and management courses.

FinTech Companies and Technology Providers

Innovation in technology should go hand in hand with consumer protection. Interface designs should feature simplicity, transparency, and security, together with explanations about permissions, authentication processes, privacy, and reporting. There should be incorporation of fraud warnings using AI that recognizes unusual behavior, while at the same time educating consumers before the transaction is completed. Updates, encryption, biometrics, and adaptive security should all continue to be standard practice, as well as in-app education that empowers consumers through activity.

Working Women

Regularly changing passwords, using multi-factor authentication, not sharing OTPs, checking the genuineness of the communication, and doing transactions on private Wi-Fi networks are some measures which individuals must take. It is crucial for statements and transaction records to be checked on a regular basis to check any sort of unauthorized activity. Individuals must use discretion while dealing with any kind of urgent requests from their clients through calls, messages, emails, and even social media. At the same time, one needs to have balance in his confidence levels and keep learning about new threats.

Towards a Digital Financial Resilience Framework

The above recommendations can contribute to a move from digital inclusion towards digital resilience – the ability to foresee, recognize, react to, and recover from any danger. In order to foster resilience, an integrated ecosystem has to be formed where the enabling framework is set up by policymakers; secure services are delivered by institutions; capability is fostered by employers; lifelong competencies are developed by educators; security is a priority for technological providers; and individuals practice safe behavior. In such an ecosystem, DFL is the fundamental capability that links knowledge with behavioral and psychological readiness.

Conclusion and Future Research Directions

Conclusion

The development of the digital economy in India has changed the manner in which financial services are accessed, delivered, and consumed. The initiatives such as Digital India, UPI, Aadhar based offerings, and FinTech have helped to enhance inclusion through convenient and accessible services. Some of the beneficiaries of this initiative have been women at work who have increased their participation and independence and thereby opted for digital transactions, banking, investments, and other products.

Nevertheless, this growth has led to a complex array of cyber risks as online fraud has shifted from being just technological based attacks to being behavioral attacks using trust, urgency, authority, fear, curiosity, and other cognitive factors apart from infrastructure issues.

This research suggests that there is a need for development in the concept of financial literacy. The financial literacy knowledge on the principles of budgeting, savings, investment, inflation, and interest rate is crucial and still needed but inadequate in the context of the digital environment. DFL needs to be understood as a multi-faceted skill that incorporates financial literacy, digital literacy, cyber-security awareness, critical analysis, and responsible behavior. One important concept of the research is that DFL is not directly protecting the consumer; it is protecting them indirectly by means of protective financial behavior. Consumers have an idea about the risk but do not take protective action because of the reasons mentioned earlier.

Confidence is further emphasized for its dual character in the paper. While considered positive traditionally, confidence is effective only if it is based on capability. The right level of confidence boosts protective behavior by enhancing self-efficacy, while overconfidence makes people less vigilant and more vulnerable. Thus, education must be designed in such a way to foster confidence and its congruence with competence. It is the focus on working women as one of the fastest-growing and most underresearched groups that makes the research cover a novel topic, showing how women experience different challenges and opportunities due to autonomy, participation, responsibilities, and new dangers. In the proposed framework, DFL, PFB, FC, and OFV are integrated into a comprehensive approach that shows how cognitive, behavioral, and psychological aspects work together influencing resilience. Practical implications include the recommendation for policymakers to reconsider educational programs that concentrate on knowledge but ignore cyber-security and behavioral capability, using collaboration and incorporating education in protection. Finally, the future of inclusion does not mean access, but secure, competent and responsible consumption of DFL as a policy target.

Limitations of the Study

Some limitations must be highlighted. Firstly, the study is theoretical and does not incorporate any empirical data, thus the relationships that have been postulated in the study are theoretically formulated instead of being statistically tested. Secondly, the topic of the paper has been discussed from the Indian perspective and specifically for women working in Delhi-NCR; the varying level of development, regulations, cultural background, and level of inclusion might influence the applicability of the suggested framework elsewhere. Thirdly, the ever-changing nature of technology and cybercrimes (e.g., advancement in artificial intelligence, deep fakes, and crypto currencies) presents the inherent limitation.

Future Research Directions

This research offers many opportunities. Firstly, it is necessary to empirically validate the proposed model using the structural equation modelling approach to establish the relationships between DFL, PFB, FC and OFV. Secondly, longitudinal studies may be carried out to find out how DFL and PFB develop together with the development of technologies. Thirdly, comparative research may be conducted among different demographics, men and women, rural and urban populations, younger and older people, people working in the public and private sectors, among those with higher and lower incomes. Fourthly, the impact of such things as AI, machine learning, biometrics, blockchain and digital identity technologies on people's protection needs to be researched. Fifthly, research can include many other psychological constructs like digital trust, perceived risk, technology readiness, self-efficacy, cognitive reflection, financial anxiety and cyber-resilience. Finally, cross-national studies can be done to understand the role of regulatory framework, culture, digital maturity, education policy in shaping cyber-resilience.

Concluding Remarks

As economies digitize, inclusion cannot simply be defined by accounts created or transactions performed. Inclusion must incorporate the necessary knowledge, awareness, behavioural ability, and judgment needed to operate safely. Working women are one of the most innovative demographic groups within India's digital economy. Building their DFL means securing household stability, consumer awareness, inclusive economic development, and national stability. By changing the perspective from adoption to resilience, this paper contributes to the discussion of behavioural finance and consumer protection, while also providing an outline for empirical research. In today's world, as more and more financial decisions are mediated through the use of technology, cultivating consumers who are digitally literate, behaviourally savvy, and cyber-aware will be crucial to making the innovation safe and beneficial.

References

1. Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211.
2. Isaia, E., Oggero, N., & Sandretto, D. (2024). Is financial literacy a protection tool from online fraud in the digital era? Journal of Behavioral and Experimental Finance, 44, 100977. https://doi.org/10.1016/j.jbef.2024.100977
3. Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology, 19(5), 469–479.
4. Mishra, D., Agarwal, N., Sharahiley, S., & Kandpal, V. (2024). Digital financial literacy and its impact on financial decision-making of women: Evidence from India. Journal of Risk and Financial Management, 17(10), 468. https://doi.org/10.3390/jrfm17100468
5. Morgan, P. J., & Huang, B. (2019). The need to promote digital financial literacy for the digital age. In The Future of Work and Education for the Digital Age. Asian Development Bank Institute (ADBI Press).
6. Nogueira, M. C., Almeida, L., & Tavares, F. O. (2025). Financial literacy, financial knowledge, and financial behaviors in OECD countries. Journal of Risk and Financial Management, 18(3), 167. https://doi.org/10.3390/jrfm18030167
7. OECD. (2018). G20/OECD-INFE policy guidance on digital financial literacy. OECD Publishing. https://doi.org/10.1787/effe2693-en
8. OECD. (2021). Digital delivery of financial education: Design and practice. OECD Publishing. https://doi.org/10.1787/d02549e7-en
9. OECD. (2021). G20/OECD-INFE report on supporting financial resilience and transformation through digital financial literacy. OECD Publishing.
10. OECD. (2024). OECD/INFE survey instrument to measure digital financial literacy. OECD Publishing. https://doi.org/10.1787/548de821-en
11. OECD. (2026). Protecting consumers from financial scams and frauds. OECD Publishing. https://doi.org/10.1787/d41817bb-en
12. Ogunola, A. A., Sonubi, T., Toromade, R. O., Ajayi, O. O., & Maduakor, A. H. (2024). The intersection of digital safety and financial literacy: Mitigating financial risks in the digital
13. economy. International Journal of Science and Research Archive, 13(1), 673–691.
14. 13. Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93–114.
15. Tan, E. (2025). Review of research on digital financial literacy: Measurement, causes, and impact. Journal of Economic Surveys. Advance online publication.

    https://doi.org/10.1111/joes.70109.

❑❑❑